The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/22/2016

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in iOS, watchOS, tvOS, Xcode, OS X El Capitan, OS X Server 5.1, and Safari, which could allow for arbitrary code execution. OS X is an operating system for Apple computers. Apple Safari is a web browser available for OS X and Microsoft Windows. Apple iOS is an operating system for iPhone, iPod touch, and iPad. watchOS is the mobile operating system of the Apple Watch. tvOS is an operating system for Apple TV digital media player. Xcode is a development environment for developing software for OS X and iOS. OS X El Capitan is an operating system for Macintosh computers.

Successful exploitation of these vulnerabilities could result in, but are not limited to information disclosure, access restricted ports on arbitrary servers, giving an attacker the ability determine kernel memory layout, or allow for arbitrary code to be run within the context of the user or kernel.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- iOS 9.3 for iPhone 4s and later, iPod touch (5th generation) and later, and iPad 2 and later
- watchOS 2.2 for Apple Watch Sport, Apple Watch, Apple Watch Edition, and Apple Watch Hermes
- tvOS 9.2 for Apple TV (4th generation)
- Xcode 7.3 for OS X El Capitan v10.11 and later
- OS X El Capitan v10.11.4 and Security Update 2016-002 for OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11 to v10.11.3
- OS X Server 5.1 for OS X Yosemite v10.10.5 and later
- Safari 9.1 for OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11 to v10.11.3

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in iOS, watchOS, tvOS, Xcode, OS X El Capitan, OS X Server 5.1, and Safari. The most serious of these vulnerabilities could lead to arbitrary code execution. Details of all vulnerabilities are as follows:

- Multiple memory corruption could allow for execution of arbitrary code with kernel privileges (CVE-2016-1733, CVE-2016-1734, CVE-2016-1735, CVE-2016-1736, CVE-2016-1743, CVE-2016-1744, CVE-2016-1746, CVE-2016-1747, CVE-2016-1748, CVE-2016-1749, CVE-2016-1754, CVE-2016-1755, CVE-2016-1759, CVE-2016-1741, CVE-2016-1717, CVE-2016-1719, CVE-2016-1720, CVE-2016-1721, CVE-2016-1722)
- Out-of-bounds read issue could allow the attacker to be able to determine kernel memory layout (CVE-2016-1732, CVE-2016-1758)
- Multiple vulnerabilities in processing various file types can lead to arbitrary code execution(CVE-2015-8126, CVE-2015-8472 ,CVE-2016-1737, CVE-2016-1740, CVE-2014-9495, CVE-2015-0973, CVE-2016-1767, CVE-2016-1768, CVE-2016-1769, CVE-2015-8126, CVE-2016-1775, CVE-2015-1819, CVE-2015-5312, CVE-2015-7499, CVE-2015-7500, CVE-2015-7942, CVE-2015-8035, CVE-2015-8242, CVE-2016-1761, CVE-2016-1762, CVE-2015-7995, CVE-2016-1740)
- A code signing verification issue could allow for execution of arbitrary code in the application's context (CVE-2016-1738)
- Multiple vulnerabilities exist that could allow a remote attacker to execute arbitrary code (CVE-2015-8659, CVE-2015-3184, CVE-2015-3187)
- A null pointer dereference may lead to denial of service (CVE-2016-1745)
- A use after free vulnerability could allow for execution of arbitrary code with kernel privileges (CVE-2016-1750)
- A race condition could allow for execution of arbitrary code with kernel privileges (CVE-2016-1757)
- A null pointer dereference could allow for execution of arbitrary code with kernel privileges (CVE-2016-1756)
- Multiple integer overflow vulnerabilities could allow for execution of arbitrary code with kernel privileges (CVE-2016-1753)
- A vulnerability exists that could lead to denial of service (CVE-2016-1752)
- A vulnerability exists when processing a JavaScript link that could reveal sensitive user information (CVE-2016-1764)
- A cryptographic vulnerability may allow an attacker who is able to bypass Apple's certificate pinning, intercept TLS connections, inject messages, and record encrypted attachment-type messages to be able to read attachments (CVE-2016-1788)
- A default setting could allow connecting to a server to expose sensitive information (CVE-2016-0777, CVE-2016-0778)
- Multiple vulnerabilities exists in LibreSSL (CVE-2015-5333, CVE-2015-5334)
- A memory leak existed in OpenSSL that could lead to denial of service (CVE-2015-3195)
- A vulnerability exists where clicking a tel link makes a call without prompting the user (CVE-2016-1770)

- A vulnerability exists that could allow a local attacker to cause unexpected application termination or arbitrary code execution (CVE-2015-7551, CVE-2016-1765)
- A permissions vulnerability exists that could allow for execution of arbitrary files (CVE-2016-1773)
- A memory corruption vulnerability could allow an attacker with a privileged network position to execute arbitrary code (CVE-2016-0801, CVE-2016-0802)
- A vulnerability when performing a server backup may cause backups to be stored on a volume without permission enabled (CVE-2016-1774)
- A vulnerability exists where an attacker may be able to exploit weaknesses in the RC4 cryptographic algorithm (CVE-2016-1777)
- A file access vulnerability could allow a remote user to view sensitive configuration information (CVE-2016-1776)
- A security bypass vulnerability exists that could allow an attacker in a privileged network position could leak sensitive user information (CVE-2016-1787)
- A vulnerability exists where visiting a malicious website may lead to user interface spoofing (CVE-2009-2197, CVE-2016-1786)
- An input validation vulnerability exists that could lead to a denial of service (CVE-2016-1771)
- Multiple vulnerabilities exist that could allow a website to track sensitive user information (CVE-2016-1772, CVE-2016-1781)
- A port redirection vulnerability exists which may allow malicious websites to access restricted ports on arbitrary servers (CVE-2016-1782)
- A vulnerability exists which could allow for a maliciously crafted site may reveal a user’s current location (CVE-2016-1779)
- A resource exhaustion vulnerability may result in an unexpected Safari crash (CVE-2016-1784)
- A caching vulnerability may allow a malicious website to exfiltrate data cross-origin (CVE-2016-1785)
- A memory corruption vulnerability could allow the attacker to be able to determine kernel memory layout (CVE-2016-1748)
- A permissions vulnerability exists that could allow an attacker to bypass code signing (CVE-2016-1751)
- A vulnerability exists in the parsing of SMS URLs which could result in other Message threads auto-filling (CVE-2016-1763)
- A certificate validation issue exists that could allow untrusted MDM profile to be displayed as verified (CVE-2016-1766)
- A vulnerability may allow a hidden webpage to track device orientation and motion (CVE-2016-1780)
- A vulnerability exists when processing web content that could lead to arbitrary code execution (CVE-2016-1723, CVE-2016-1724, CVE-2016-1725, CVE-2016-1726, CVE-2016-1727, CVE-2016-1778, CVE-2016-1783)
- A vulnerability exists when processing maliciously crafted certificates that could lead to arbitrary code execution (CVE-2016-1950)

Successful exploitation of these vulnerabilities could result in but not limited to information disclosure, access restricted ports on arbitrary servers, give an attacker the ability determine kernel memory layout, or allow for arbitrary code to be run within the context of the user or kernel.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:
https://support.apple.com/en-us/HT206166
https://support.apple.com/en-us/HT206168
https://support.apple.com/en-us/HT206169
https://support.apple.com/en-us/HT206172
https://support.apple.com/en-us/HT206167
https://support.apple.com/en-us/HT206173
https://support.apple.com/en-us/HT206171

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2197
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9495
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0973
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1551
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3184
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3187
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3195
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5312
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5333
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5334
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7499
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7500
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7942
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7994
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8035
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8126
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8242
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8472
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8659
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0778
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0801
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0802
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1717
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1719
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1720
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1721
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1722
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1723

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1724
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1725
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1726
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1727
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1732
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1733
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1734
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1735
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1736
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1737
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1738
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1740
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1741
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1743
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1744
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1745
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1746
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1747
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1748
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1749
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1750
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1751
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1752
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1753
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1754
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1755
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1756
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1757
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1758
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1761
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1762
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1763
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1764
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1765
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1766
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1767
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1768
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1769
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1770
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1771
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1772
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1773
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1774
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1775
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1776
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1777
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1778
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1779

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1780
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1781
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1782
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1783
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1784
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1785
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1786
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1787
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1788
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1819
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1950
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8126